Tidecoin : A Post-Quantum Security Peer-to-peer Crypto Cash

EverettX

tidecoin.org

Dec 10, 2020

Abstract. By introducing the Post-Quantum security signature algorithm, a decentralized currency system Tidecoin is designed. The operation of the Tidecoin network is based on mathematical proofs and physical laws. The proof of power consensus and CPU friendly POW algorithm make Tidecoin achieving a breakthrough level in decentralization, and security. The currency design enables Tidecoin to run on various types of ubiquitous computing devices, enabling pervasive process of value, even that in multiple worlds.

1. Introduction

Bitcoin [1] is a distributed peer-to-peer electronic payment system maintained by proof of computing power. It can enable any two parties to reach an agreement to pay directly without the participation of a third-party intermediary on the Internet. This technology of Bitcoin is now called blockchain. It is completely based on the principles of cryptography. Proof of work can guarantee that as long as the accumulation of the hash work controlled by honest nodes is greater than the accumulation of the attacker's, the system is safe.

This technology avoids the need to use financial institutions as a trusted third party to process electronic payment information in a credit-based model, which can reduce transaction costs and avoid the vulnerability of intermediaries. In addition to payment functions, through limited programming scripts, Bitcoin can implement more complex applications such as multi-signature fund management and e-commerce, etc.

However, due to the progressing of quantum computer technology, bitcoin's core crypto algorithm ECDSA is facing the great threat of Quantum computing power. 09/Dec/2020, "Photonic Quantum Computer Displays 'Supremacy' Over Supercomputers", a news from spectrum.ieee.org. It clearly shows that billions value on bitcoin network is facing the threat of Quantum computers. It is time to build a Post-Quantum security cryptocurrency.

Tidecoin is a peer-to-peer Internet currency that enables instant, near-zero cost payments to anyone in the world. Tidecoin is an open source global payment network, and fully decentralized without any central authorities. Features of Post-Quantum security make Tidecoin as a replacement to Bitcoin. Tidecoin's new cryptography algorithm of Falcon is an lattice-based cryptography algorithm and based on the theoretical framework of Gentry, Peikert and Vaikuntanathan. There is no efficient solving algorithm currently known in the

general case, even with the help of quantum computers, because the underlying hard problem is the short integer solution problem (SIS) over NTRU lattices.

2. Post-Quantum security signature algorithm

Falcon - Fast-Fourier Lattice-based Compact Signatures over NTRU. Falcon follows a framework introduced in 2008 by Gentry, Peikert, and Vaikuntanathan, the high-level idea is the following:

The public key is a long basis of a q-ary lattice. The private key is (essentially) a short basis of the same lattice.

In the signing procedure, the signer:

a. Generates a random value salt

b. Computes a target **c=H(msg||salt)**, where **H** is a hash function sending an input to a random-looking point (on the grid)

c. Uses his knowledge of a short basis to compute a lattice point **v** close to the target **c**

d. Outputs **(salt, s)**, where **s=c−v**

In the verifying procedure, The verifier accepts the signature **(salt, s)**

a. if and only if the vector s is short

b. **H(msg||salt) −s** is a point on the lattice generated by his public key.

Falcon offers the following features:

- Security: a true Gaussian sampler is used internally, which guarantees negligible leakage of information on the secret key up to a practically infinite number of signatures (more than 264). To give a point of comparison, Falcon-512 is roughly equivalent, in classical security terms, to RSA-2048, whose signatures and public keys use 256 bytes each.
- Compactness: thanks to the use of NTRU lattices, signatures are substantially shorter than in any lattice-based signature scheme with the same security guarantees, while the public keys are around the same size.
- Speed: use of fast Fourier sampling allows for very fast implementations, in the thousands of signatures per second on a common computer; verification is five to ten times faster.
- Scalability: operations have cost O (n log n) for degree n, allowing the use of very long-term security parameters at moderate cost.

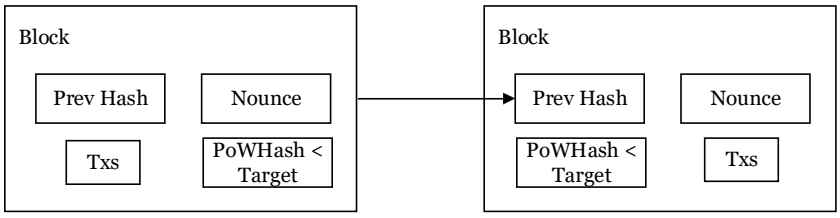
- RAM Economy: the enhanced key generation algorithm of Falcon uses less than 30 kilobytes of RAM, a hundredfold improvement over previous design such as NTRU Sign. Falcon is compatible with small, memory-constrained embedded devices.

Choice Falcon as the replace signature of bitcoin is one of the best. In fact, There is no efficient solving algorithm currently known in the general case, even with the help of quantum computers, because the underlying hard problem is the short integer solution problem (SIS) over NTRU lattices. So the Tidecoin network is based on mathematical proof and physical laws, due to its provable theory. The security is the most important value as a cryptocurrency.

3. Proof of work (PoW) consensus

Proof of work(PoW), is a consensus algorithm that can be separated from a specific physical basis, a calculation process that can be trusted by any third party, and a completely decentralized consensus system whose decentralization degree is largest.

The PoW algorithm used by Tidecoin is yespower, a cpu friendly mining algorithm. Yespower is builds upon scrypt. This algorithm is CPU-friendly, GPU-unfriendly, and FPGA/ASIC-neutral. In other words, it's meant to be relatively efficient to compute on current CPUs and relatively inefficient on current GPUs. The production of workload is related to physical laws and driven by productivity. It guarantees the security of Tidecoin network is protected by computing power.



PoW algorithm is working as follows.

1) The full node performs HASH calculations on the block header variables:

   H (Nonce) = Hash (Hash (nVersion, hashPrevBlock, hashMerkleRoot, nTime, nBits, Nonce))

2) nBits defines the difficulty of proof of work, and PoWTARGET can obtain trough nBits

3) Compare the generated H (Nonce) and PoWTARGET

   If H (Nonce) < PoWTARGET, then

   POW is valid

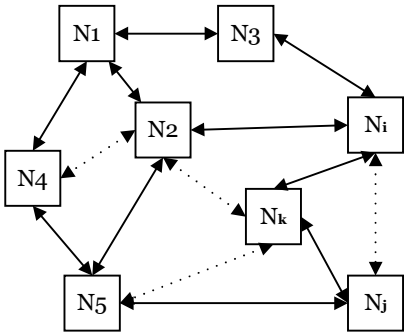
4) Then the full node can broadcast new block to the network, and can get a block reward

5) If and only if the more than 51% full node collects the valid POW block, and added to the top of the longest chain, the block is confirmed by network

In summary, PoW consensus algorithm makes the network only depends on the mathematical proof of work but not any third party.

4. Network

The point-to-point network on the Tidecoin network does not require super nodes, and each full node runs the same configuration and code. The topology of the network is constructed by broadcasting, which forms a self-organizing network. There can be direct links between network nodes for two-way communication, or point-to-point connective path through routing. Both the link and the route are generated in a decentralized network protocol.



The consensus system is running through the point-to-point network. The main processes in a full node are:

1) The new transaction will be broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node performs the POW and broadcasts it to the network if the proof is valid
4) Each node collects proof of work into blocks
5) When the node collects the proof of work it generates a valid block and propagates it to all nodes.
6) Only when POW and all the transactions in it are valid, the node accepts the block.
7) The node expresses the acceptance chain of the block by creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes accumulate the proved work of the chain, and always regard the chain with the longest accumulated proof as the correct chain, and will continue to work hard to expand

it. If two nodes broadcast different versions of the next block at the same time, some nodes may receive one or the other first. In this case, they will process the first block received, but save another branch in case it becomes longer. The next time a block is generated, the blocks with the most proved work and stake will win and become a longer branch; this way most nodes on the network will switch to the longest branch.

5. Conclusion

We reviewed the experimental results of Bitcoin in the decentralized cash system, and clarified the core of the decentralized cash system: decentralization, security, and scalability. To this end, we have designed a cash system Tidecoin based on Post-Quantum security crypto algorithm. The Tidecoin network is based on mathematical proof and physical laws, which ensures its decentralization and security nature. The script system to scale the network by programmable code or sidechains.

6. References

1. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.
2. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU, https://falcon-sign.info/falcon.pdf
3. https://spectrum.ieee.org/tech-talk/computing/hardware/photonic-quantum-computer-shows-advantage-over-supercomputer
4. J. Poon and T. Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2015.
5. https://www.openwall.com/yespower/
6. A Back. Enabling Blockchain Innovations with Pegged Sidechains, 2014
7. Weiser, Mark. Some Computer Science Issues in Ubiquitous Computing,1993